Warszawa, 21.10.2019 r.

Informacja prasowa

**Jak przygotować się do kontroli UODO?**

**Tylko w 2018 roku przeprowadzono łącznie 72 kontrole przestrzegania przepisów o ochronie danych osobowych – wynika ze sprawozdania UODO. Do sierpnia 2019 r. ta liczba wzrosła do 113. Prezes Urzędu Ochrony Danych Osobowych ma prawo przeprowadzić kontrolę w każdej organizacji – zarówno z sektora prywatnego, jak i publicznego. Jak odpowiednio się do niej przygotować? Ekspert z ODO 24 podpowiada, na co zwrócić uwagę.**

**Kontrola – co warto wiedzieć?**

Wyróżniamy trzy rodzaje kontroli (art. 78 ust. 2 u.o.d.o.): kontrolę planową – na podstawie zatwierdzonego planu kontroli organu nadzorczego, doraźną – na podstawie informacji uzyskanych przez Prezesa UODO oraz wyrywkową (w ramach monitorowania przestrzegania RODO, zależną od swobodnego wyboru Prezesa UODO).

Z założenia organ powinien poinformować daną organizację o kontroli. Samo RODO jednak nic o tym nie mówi, wynika to natomiast z ustawy Prawo przedsiębiorców. Zgodnie z jej art. 48 organ przystępujący do kontroli zawiadamia przedsiębiorcę o jej zamiarze. Rozpoczyna się ją nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia.

*Należy jednak pamiętać, że ustawa Prawo przedsiębiorców przewiduje wyjątki, kiedy organ nie zawiadamia o kontroli. Przykładowo obejmują one sytuacje, kiedy jej przeprowadzenie jest niezbędne dla przeciwdziałania popełnieniu przestępstwa (wykroczenia) lub zabezpieczenia dowodów jego popełnienia, a także gdy przedsiębiorca nie ma adresu zamieszkania lub adresu siedziby lub doręczanie pism na podane adresy było bezskuteczne lub utrudnione* – wskazuje Agata Kłodzińska, ODO 24.

**Zakres kontroli**

Zakres kontroli, którą objęte zostanie przetwarzanie danych osobowych w danej organizacji, najczęściej wskazany jest w treści zawiadomienia. Zazwyczaj możemy liczyć na ogólne określenie procesu, który ma zostać poddany sprawdzeniu, np. przetwarzanie danych osobowych pracowników, proces związany z marketingiem czy stosowany przez organizację monitoring.

*Równie dobrze przedmiot kontroli może dotyczyć całości podejmowanych przez organizację czynności przetwarzania albo pewnego aspektu rozpatrywanego w ramach kilku (lub wszystkich) procesów przetwarzania (np. prowadzenie monitoringu wizyjnego w organizacji czy realizacja obowiązku informacyjnego). Warto po otrzymaniu zawiadomienia skontaktować się z urzędnikiem i spróbować pozyskać bardziej precyzyjne informacje w tym zakresie. Natomiast drugim dokumentem, z którego wynika, jakie zagadnienia zostaną poddane sprawdzeniu przez kontrolerów, jest imienne upoważnienie pracownika UODO –* mówi Agata Kłodzińska, ODO 24.

**Dzień odwiedzin**

Gdy nadejdzie wyznaczony dzień kontroli warto, aby administrator oczekiwał na osoby wyznaczone do jej przeprowadzenia. *Co ważne, przed umożliwieniem podjęcia czynności kontrolnych należy upewnić się, że osoby, które podają się za uprawnione do kontroli, rzeczywiście mają pełne prawo do jej przeprowadzenia. Obowiązkowo należy zweryfikować imienne upoważnienie do kontroli oraz legitymację służbową, której wzór znajduje się w rozporządzeniu Rady Ministrów z 20.03.2019 r. w sprawie wzoru legitymacji służbowej pracownika UODO* – dodaje Agata Kłodzińska, ODO 24.

Najczęściej kontrola jest przeprowadzana w składzie kilkuosobowym: w większych organizacjach trzy osoby, w mniejszych dwie osoby, przy czym jeden z kontrolerów odpowiada za obszar prawny, a drugi – za kwestie zabezpieczeń technicznych, fizycznych i organizacyjnych, w tym szeroko pojęte zagadnienia związane z IT.

Dobrze jest również wiedzieć, jakie obowiązki ciążą na kontrolujących i kontrolowanym, a także jakie prawa im przysługują. Przede wszystkim w ramach prowadzonych czynności kontrolnych kontrolujący ma prawo do (art. 84 ust. 1 u.o.d.o.) m.in.: wglądu do dokumentów mających bezpośredni związek z przedmiotem kontroli; przeprowadzenia oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych; żądania złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwania świadków (np. pracowników kontrolowanego). Z kolei kontrolowany ma obowiązek umożliwić kontrolerom UODO sprawne przeprowadzenie kontroli, w związku z czym oprócz aktywnego w niej udziału i odpowiedzi na pytania zadawane w trakcie czynności kontrolnych może być zobowiązany do sporządzania kopii lub wydruków zarówno dokumentów, jak i informacji zgromadzonych na nośnikach, urządzeniach i w systemach.

Po zakończeniu czynności kontrolnych oraz całego procesu organ nadzorczy dokonuje analizy zgromadzonego materiału dowodowego. Jeśli uzna, że mogło dojść do naruszenia przepisów o ochronie danych, niezwłocznie wszczyna postępowanie administracyjne.

**Case study:**

**Milion za niezgodność**

**Problem:** Niespełnienie obowiązku informacyjnego w stosunku do osób prowadzących jednoosobowe działalności gospodarcze (JDG), których dane znalazły się w bazach spółki tworzącej bazy danych przedsiębiorców w oparciu o ogólnodostępne źródła takie jak CEiDG, KRS czy GUS.

**Działanie:** Spółka podjęła działania zmierzające do spełnienia obowiązku informacyjnego. Opublikowała stosowną klauzulę na stronie WWW i przeprowadziła masową wysyłkę mailową z informacjami na temat przetwarzania danych do wszystkich osób, których adresami mailowymi dysponowała (łącznie ok. 680 tysięcy rekordów). Natomiast w stosunku do reszty osób – zrezygnowała ze spełnienia obowiązku informacyjnego, powołując się na niewspółmiernie duży wysiłek związany z przekazaniem im klauzuli informacyjnej tradycyjną drogą pocztową.

**Rozwiązanie:** Zdaniem UODO administrator podjął pewne, choć niewystarczające kroki w kierunku zgodności z RODO, w związku z czym w oparciu o ustalenia poczynione w trakcie kontroli Prezes UODO ukarał warszawską spółkę. W tej sprawie UODO dokonał interpretacji pojęcia „niewspółmiernie dużego wysiłku”, stwierdzając, że wysyłka ok. 6 milionów listów poleconych z klauzulami informacyjnymi (bo w odniesieniu do tylu osób spółka dysponowała wyłącznie adresem prowadzenia działalności) takim niewspółmiernie dużym wysiłkiem wcale by nie była, gdyż nie chodzi o skalę wysiłku dla podmiotu, a raczej o wysiłek związany z jednostkowym poinformowaniem osoby. Przykładowo niewspółmiernie dużym wysiłkiem byłoby ustalanie adresów kontaktowych osób, które podały jedynie imię, nazwisko i numer PESEL, bez adresu zamieszkania, korespondencji czy numerów telefonu.

**ODO 24 sp. z o. o.** oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z zakresu m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

Kontakt dla mediów:

**Triple PR**

**Aneta Gałka**

tel. 570 533 678

aneta.galka@triplepr.pl